# 《信息安全新技术》

## 图书基本信息

书名：《信息安全新技术》

13位ISBN编号：9787563533572

10位ISBN编号：7563533575

出版时间：2013-1

出版社：杨义先、马春光、钮心忻、 孙建国 北京邮电大学出版社 (2013-01出版)

页数：232

# 《信息安全新技术》

## 内容概要

《信息安全专业系列教材:信息安全新技术(第2版)》对国内外网络信息安全方面有代表性的最新技术作了系统而详细的总结。《信息安全专业系列教材:信息安全新技术(第2版)》共10章，分别对信息隐藏技术、数字水印技术、多媒体信息伪装技术、入侵检测技术、电子支付技术、网络安全协议、智能卡安全技术、公钥基础设施（PKI）、物联网安全和无线网络安全技术等进行了充分的论述。

# 《信息安全新技术》

## 书籍目录

# 《信息安全新技术》

## 章节摘录

版权页： 插图： （1）隐写术：一般指那些进行秘密通信的技术的总称，通常把秘密信息嵌入或隐藏在其他不易受怀疑的数据中。伪装方法通常依赖于第三方不知道隐蔽通信的存在的假设，而且主要用于互相信任的双方的点到点秘密通信。因此，隐写术一般稳健性较弱。例如：在数据改动后隐藏的信息不能被恢复。 （2）数字水印：数字水印就是向被保护的数字对象（如静止图像、视频、音频等）嵌入某些能证明版权归属或跟踪侵权行为的信息，可以是作者的序列号、公司标志、有意义的文本等等。同隐写术相反，水印中的隐藏信息具有能抵抗攻击的稳健性。即使知道隐藏信息的存在，对攻击者而言，要毁掉嵌入的水印仍很困难（理想的情况是不可能），虽然水印算法的原理是公开的。在密码学中，这就是众所周知的Kerkhoffs原理：加密系统在攻击者已知加密原理和算法但不知道相应的密钥的仍是安全的。稳健性的要求使得水印算法中在宿主数据中嵌入的信息要比隐写术中要少。水印技术和隐写术更多的时候是互补的技术而不是互相竞争的。 （3）数据隐藏和数据嵌入：通常用在不同的上下文环境中，它们一般指隐写术，或者指介于隐写术和水印之间的应用，在这些应用中嵌人数据的存在是公开的，但没必要保护它们。例如：嵌人的数据是辅助的信息和服务，它们可以是公开得到的，与版权保护和控制存取等功能无关。 （4）指纹和标签：指水印的特定用途。有关数字产品的创作者和购买者的信息作为水印而嵌入，每个水印都是一系列编码中的唯一的一个编码，即水印中的信息可以唯一地确定每一个数字产品的拷贝，因此，它们被称为指纹或者标签。 1.2 信息隐藏的基本手段 信息隐藏（或称为信息伪装）的手段非常多，从隐藏信息的载体来看，有以下几种。 （1）在文本中隐藏信息 利用语言的自然冗余性，将信息直接编码到文本内容中去；或者将信息直接编码到文本格式中去（比如，调整字间距或行间距）；如果载体文本以固定格式（像HTML、LATEX或Postscript文件）的形式传输，则信息可以嵌入到格式中而不是消息内容本身，秘密信息可以存储在行间距或列间距中，如果两行之间的距离小于某个门限值，就表示隐藏的信息是“0”，否则隐藏的信息是“1”（类似的方法也可用于传输ASCII码文本的信息：偶尔的附加空格字符可以用来构成秘密信息）；将信息编码隐藏在字处理系统的断行处。 在文本消息中能否存在安全和健壮的信息隐藏仍然是一个悬而未决的问题。一个攻击者只需简单地重新调整文本的格式，就可以破坏掉所有嵌入在文本格式中的信息。另外，文本消息可以以各种不同的格式进行存储（像HTML、TEX'sDVI、Postscript、PDF，或者RTF），从一种格式转化到另一种格式对嵌入的消息也有很大的损害。

# 《信息安全新技术》

## 编辑推荐

《信息安全专业系列教材:信息安全新技术(第2版)》内容翔实，叙述通俗易懂。可作为通信与电子系统、信号与信息处理、密码学、信息安全、计算机应用等专业的研究生、本科生和大专生相关课程的教学参考书。也可作为从事国家网络信息安全工作人员提高业务水平的实用工具书。同时，《信息安全专业系列教材:信息安全新技术(第2版)》也可作为国内网络安全、计算机安全和信息安全领域相关人员的技术培训教材。

# 《信息安全新技术》

## 版权说明